(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 101 10 316 A 1**

(51) Int. Cl.[7]:
G 06 F 12/14
H 04 L 9/32

(21) Aktenzeichen: 101 10 316.6
(22) Anmeldetag: 3. 3. 2001
(43) Offenlegungstag: 27. 9. 2001

DE 101 10 316 A 1

(30) Unionspriorität:
001055284 15. 03. 2000 EP

(71) Anmelder:
International Business Machines Corp., Armonk, N.Y., US

(74) Vertreter:
Gigerich, J., Dipl.-Ing., Pat.-Ass., 70563 Stuttgart

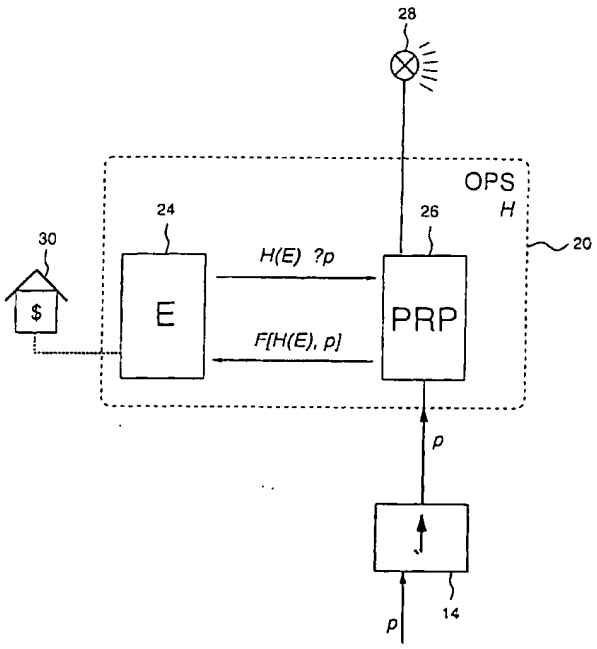
(72) Erfinder:
Riordan, James, Adlisil, CH

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Sichere Passworteingabe

(57) Die Erfindung sieht eine Einrichtung für eine sichere Passworteingabe durch Verwendung von kryptographischen Funktionen vor. Diese Einrichtung ist beim Zugriff auf Computer und Programme anzuwenden. Nach einer Anforderung vom Programm E wird ein Passwort p eingelesen, indem ein programmspezifisches Identifizierungszeichen H(E) vom Programm E empfangen wird, das das Passwort p empfängt und wenigstens von dem programmspezifischen Identifizierungszeichen H(E) und dem empfangenen Passwort p ein programm-passwortspezifisches Identifizierungszeichen F(H(E), p) erzeugt wird. Das programm-passwortspezifische Identifizierungszeichen F(H(E), p) wird an das Programm E gesendet, das dann das programm-passwortspezifische Identifizierungszeichen F(H(E), p) weiterverarbeitet.



DE 101 10 316 A 1

Beschreibung

TECHNISCHER BEREICH

Die vorliegende Erfindung bezieht sich auf eine sichere Passworteingabe. Die Erfindung bezieht sich insbesondere auf ein Verfahren und ein Gerät, um ein Passwort auf sichere Art und Weise einzulesen.

HINTERGRUND DER ERFINDUNG

Passwörter und Passwortschutzschemata werden gemeinhin benutzt, um Zugriff auf Computersysteme und -programme zu erhalten. Jedesmal, wenn ein Benutzer den Computer oder das Programm benutzen möchte, wird er bzw. sie aufgefordert, ein Passwort einzugeben. Ist das Passwort gültig, darf der Benutzer auf die Daten zugreifen bzw. die Programme ausführen. Personen, die kein gültiges Passwort eingeben, wird der Zugriff auf Daten oder Programminformationen verweigert. Auf diese Weise sollte ein Passwortschutzsystem die eigenen oder vertraulichen Informationen, die im Computer gespeichert sind, schützen und die unberechtigte Nutzung verhindern.

Da ein Benutzer mit mehreren Computern und Programmen arbeitet, muss er sich viele Passwörter merken. Viele neigen dazu, Passwörter versehentlich oder absichtlich wieder zu verwenden, was zu Sicherheitsproblemen führt.

Die meisten Personalcomputer (PCs) und Laptops können das Sicherheitsproblem nicht hinreichend lösen, indem sie lediglich nach einem Passwort fragen. PC-Betriebssysteme, die mit moderner Hardware einschließlich DOS, Windows und MacOS laufen, wurden von einer Virusinvasion, von Trojanischen Pferden und anderer heimtückischer Software, auch Malware (malicions software) genannt, überrannt. Freigabe und Benutzung solcher Malware sind im wesentlichen eine Form des Vandalismus und seine Gefahr nimmt mit der Benutzung des Internets zu. Das Sicherheitsrisiko, die oben erwähnten Trojanischen Pferde herunterzuladen, wird immer größer, breitet sich immer mehr aus und wird oft unterschätzt. Solche Trojanischen Pferde sind heimtückische Dateien oder Programme, die, wenn sie ausgeführt werden, als gutartige Anwendung maskiert sind, und Programme oder sogar das gesamte System kontrollieren könnten. Andere heimtückische Programme versuchen, Anmeldenamen und Passwörter zu stehlen. Diese Passwörter werden dann oft an anonyme E-Mail-Adressen geschickt. Ein Trojanisches Pferd ist im allgemeinen ein Programm, das sich fälschlicherweise selbst so darstellt, als würde es nützliche Dienste leisten.

Tatsache ist, dass der Benutzer oft nicht genau weiss, ob er bzw. sie das Passwort in das richtige System oder Programm eingegeben hat. In einem weiteren sicherheitsproblematischen Beispiel zeigt der Bildschirm beim Einschalten des Computers die Anzeigedaten an, die im Bildspeicher gespeichert sind. Daher kann jedermann Informationen zu der unterbrochenen Datenverarbeitung aus den Anzeigedaten erhalten, die im Hintergrund des Passworteingabefensters angezeigt werden. Anders ausgedrückt, kann ein unberechtigter Benutzer die Informationen ohne Eingabe eines Passworts erhalten. Für einen unberechtigten Benutzer ist es andererseits möglich, das registrierte Passwort in vielen Systemen herauszufinden, indem er wiederholt ein zufällig ausgewähltes Passwort eingibt.

Der Größenfaktor und die Verwendungsmerkmale von Handgeräten, zum Beispiel persönliche digitale Assistenten (Personal Digital Assistants), kurz PDAs genannt, machen ihren Einsatz in E-Commerce-Anwendungen sehr attraktiv. Das vorteilhafteste Merkmal dieser PDAs liegt darin, dass

jedermann sie problemlos durch einfache Bedienung an jedem beliebigen Platz nutzen kann. Andererseits wird durch die weite Verbreitung der PDAs die Möglichkeit größer, dass geheime Informationen verarbeitet werden. Deshalb sind ausreichende Betrachtungen im Hinblick auf die Sicherheitsfunktion notwendig. Normalerweise wird die Sicherheitsfunktion dadurch erreicht, dass der PDA so programmiert wird, dass bei jedem Einschalten die Passworteingabe geprüft wird. Bei dieser Passwortprüfung wird die Eingabe eines Passworts unmittelbar nach dem Einschalten verlangt. Anschließend wird geprüft, ob das eingegebene Passwort mit einem zuvor registrierten Passwort übereinstimmt. Bei übereinstimmenden Passwörtern beginnt der PDA oder Personalcomputer nach einer vom Bediener eingegebenen Anweisung mit der Datenverarbeitung. Leider bieten die aktuellen PDA-Betriebssysteme nicht die notwendige Sicherheit für E-Commerce-Anwendungen. Tatsache ist, dass die PDAs leistungsfähig sind und die Universalrechner sie für Angriffe anfällig machen. Auf PDAs basierende E-Commerce-Systeme sind möglicherweise für eine ganze Reihe von Angriffen anfällig, durch die auch andere integrierte Systeme, zum Beispiel Chipkarten, gefährdet werden können.

Wenn man diese Systeme für wirtschaftlich bedeutungsvolle Transaktionen benutzt, bedeutet dies einen weit größeren Nutzen und somit für einen Angreifer einen größeren Anreiz. Es besteht daher ein wesentlicher Bedarf an Sicherheit, wodurch sich die Nachfrage nach einem geeigneten, sicheren Passworteingabesystem ergibt.

Die US Patentschrift Nr. 5,931,948 bezieht sich auf ein tragbares Computersystem mit Passwortkontrollmitteln zum Behalten von einem oder mehreren Passwörtern, so dass die Passwörter bei direktem Zugriff von einem Hauptrechner unlesbar sind.

In der US Patentschrift Nr. 5,091,939 werden ein Verfahren und eine Vorrichtung zum Passwortschutz eines Computers beschrieben. Darin wird die Passworteingabe des Benutzers mit dem Wert eines zweiten Passworts, das vom Computer behalten wird, und dem Wert des vom Benutzer gespeicherten ersten Passworts verglichen. Der Benutzer kann somit auf den Computer zugreifen, wenn sein erstes Passwort falsch ist, oder er es vergessen hat, indem er vom Computerhersteller ein alternatives Passwort erhält, das zu dem zweiten, vom Computer generierten oder gespeicherten zweiten Passwort passt. Die Funktion des Verfahrens und der Aufbau der Vorrichtung sorgen dafür, dass die zweiten und alternativen Passwörter für eine begrenzte Zeit gültig sind und somit die volle Integrität des Passwortschutzsystems erhalten bleibt.

GEGENSTAND DER ERFINDUNG

Es ist ein Gegenstand der vorliegenden Erfindung, die Nachteile im Stand der Technik zu überwinden und Sicherheit von passwortgeschützten Computern und Programmen zu verbessern.

Es ist ein weiterer Gegenstand der vorliegenden Erfindung, ein sicheres Passworteingabesystem bereitzustellen, das heimtückische Programme entlarvt, wie zum Beispiel Trojanische Pferde, und ihre Ausführung verhindert.

Es ist noch ein weiterer Gegenstand der vorliegenden Erfindung zu erreichen, dass ein eingegebenes Passwort so codiert wird, dass es unmöglich ist, dieses Passwort wiederzufinden.

Es ist ein weiterer Gegenstand der vorliegenden Erfindung zu erreichen, dass ein Benutzer sich an das Passwort zu erinnern hat und nur ein Passwort für mehrere Computer oder Programme anwendet, da dies Sicherheit bietet.

Es ist noch ein weiterer Gegenstand der vorliegenden Erfindung, einen Personalcomputer bereitzustellen, der ein Passwort sicher einlesen kann.

GLOSSAR

Im folgenden sind informelle Definitionen aufgeführt, die zum Verständnis der nachstehenden Beschreibung beitragen.

Die Hash-Funktion ist eine wirksame Computerfunktion, die binäre Zeichenketten von beliebiger Länge als binäre Zeichenketten in fester Länge abbildet.

Die One-Way-Hash-Funktion ist eine Funktion, die eine Meldung M oder einige Daten mit variabler Länge nimmt und einen Festlängenwert errechnet, auch Hash-Identifizierungszeichen oder spezifisches Identifizierungszeichen genannt. Für ein gegebenes spezifisches Identifizierungszeichen ist es computertechnisch nicht möglich, eine Meldung mit diesem spezifischen Identifizierungszeichen zu finden. Tatsächlich kann man mit diesem spezifischen Identifizierungszeichen keine brauchbaren Informationen über die Meldung M finden. Anders ausgedrückt, braucht es wesentlich weniger Zeit, ein solches spezifisches Identifizierungszeichen zu erstellen als die Meldung mit variabler Länge aus dem spezifischen Identifizierungszeichen zu rekonstruieren. Außerdem dauert es wesentlich länger, zwei identische spezifische Identifizierungszeichen zu finden als ein spezifisches Identifizierungszeichen zu erstellen.

Die Trusted Computing Base (TCB) bezeichnet alle Schutzsysteme innerhalb eines Computersystems, einschließlich Hardware, Firmware und Software, die in der Kombination für die Unterstützung einer Sicherheitsstrategie verantwortlich sind.

ZUSAMMENFASSUNG UND VORTEILE DER ERFINDUNG

Die Gegenstände der Erfindung werden durch die in den beiliegenden unabhängigen Ansprüchen aufgeführten Merkmale erreicht. Weitere vorteilhafte Implementierungen und Ausführungsbeispiele der Erfindung sind in den jeweiligen Unteransprüchen beschrieben.

Die Erfindung stellt ein allgemeines und flexibles System für eine sichere Passworteingabe bereit. Dieses System ist auf den Zugriff von Computern und Programmen anwendbar. Wenn auf einen Computer Bezug genommen wird, ist jede Art von Computer gemeint, der eine Trusted Computing Base, kurz TCB genannt, hat. Ein solcher Computer kann Mitglied eines Netzwerks sein und mehrere sichere Domänen (domains) oder Anwendungen unterstützen.

Die Grundidee der Erfindung ist, dass ein Computer eine kryptographische Funktion benutzt, um das eingegebene Passwort in einen im wesentlichen einzigartigen Namen zu konvertieren, wobei eine sichere Passworteingabe von der Trusted Computing Base unterstützt und dem Benutzer durch ein Signal – vorzugsweise ein optisches Signal – angezeigt wird.

Eine solche kryptographische Funktion kann eine kryptographische Kontrollsumme sein, auch One-Way-Hash-Funktion genannt, um automatisch ein programmspezifisches Identifizierungszeichen von einem Programm, welches ein Passwort verlangt, und ein sogenanntes programm-/passwortspezifisches Identifizierungszeichen von dem programmspezifischen Identifizierungszeichen und dem eingegebenen Passwort zu erzeugen. Diese Identifizierungszeichen oder Namen werden durch die Anwendung einer Hash-Funktion erhalten. Die Namen werden im allgemeinen von der Trusted Computing Base oder genauer gesagt von einem Betriebssystem erzeugt, wobei ein Generatormodul eingesetzt wird. Die kryptographische Funktion erfüllt wenigstens die folgenden Kriterien. Es braucht wesentlich weniger Zeit, solch ein spezifisches Identifizierungszeichen zu erstellen als das Programm oder Teile davon aus dem spezifischen Identifizierungszeichen zu rekonstruieren. Außerdem dauert es wesentlich länger, zwei identische spezifische Identifizierungszeichen zu finden als ein spezifisches Identifizierungszeichen zu erstellen.

Der Ablauf ist wie folgt. Das Programm, das ein Passwort verlangt, sendet eine Meldung, in der wenigstens sein erzeugtes programmspezifisches Identifizierungszeichen enthalten ist an ein Passwortleseprogramm, das vom Betriebssystem bereitgestellt wird. Das Passwortleseprogramm fragt nach einem Passwort, und während dieses Programm das Passwort einliest, wird dem Benutzer ein sicherer Eingabemodus signalisiert. Das programmspezifische Identifizierungszeichen wird dann zusammen mit dem empfangenen Passwort in das programm-/passwortspezifische Identifizierungszeichen umgewandelt. Dieses umgewandelte Identifizierungszeichen wird an das Programm gesendet, das es als das angeforderte Passwort verarbeitet oder weiterleitet.

Das vorliegende System zeichnet sich durch eine Reihe von Vorteilen aus. Es kann weder verfälscht noch durchschnüffelt oder verschleiert werden. Das System beseitigt außerdem das Problem der Trojanischen Pferde und ermöglicht es, dass jeder Anwendung oder jedem Programm, die bzw. das ein Passwort verlangt, ein einziges Passwort gegeben wird, während sich der Benutzer nur ein Passwort merken muß. Anders ausgedrückt, kann ein einzelnes Passwort auf eine völlig sichere Art und Weise von mehreren verschiedenen Anwendungen oder Programmen gemeinsam benutzt werden. Die Vertrauenswürdigkeit von Computern kann im allgemeinen erheblich verbessert werden, und sie können zu sicheren und zuverlässigen Geräten gemacht werden. Daher können mehrere Domänen oder Anwendungen im selben Computer laufen, ohne dass sie von ungesicherten Programmen angegriffen werden können.

Durch den Einsatz dieses Systems können unkontrollierte und möglicherweise ungesicherte Programme, wie zum Beispiel verdächtige und angreifende Programme, keine Kontrolle über den Computer erlangen oder die empfindlichen Programme oder Daten stören.

Wenn das programmspezifische Identifizierungszeichen abgeleitet wurde, indem eine erste kryptographische Funktion auf das Programm angewendet wird, das ein Passwort verlangt, und das programm-/passwortspezifische Identifizierungszeichen erzeugt wird, indem eine zweite kryptographische Funktion auf das programmspezifische Identifizierungszeichen und wenigstens ein Teil des empfangenen Passworts angewendet wird, dann hat das den Vorteil, dass ein im wesentlichen einzigartiger Wert, der betrachtet werden kann, als konvertiertes, im wesentlichen einzigartiges Passwort bereitgestellt werden kann. Dies ist nur von dem Programm verwendbar, das das Passwort angefordert hat.

Die erste kryptographische Funktion bzw. die zweite kryptographische Funktion enthält vorzugsweise eine One-Way-Hash-Funktion, beispielsweise MD5 oder SHA-1. Dennoch können die angewendeten Hash-Funktionen auch identisch sein. Diese Hash-Funktionen sind bekannt, arbeiten zuverlässig und können verarbeitet werden, d. h. im Millisekundenbereich auf Daten oder Programme angewendet werden, ohne bemerkenswerte Auswirkungen auf den Benutzer oder die Rechenzeit im allgemeinen zu haben. Es ist auch möglich, die kryptographische Funktion auf wenigstens einen Teil des Programmcodes oder der Daten anzuwenden.

Es hat sich bewährt, wenn das Passwortleseprogramm

und das programmspezifische Identifizierungszeichen mittels einer Trusted Computing Base (TCB) – für beide vorzugsweise dieselbe TCB – bereitgestellt werden, da dann der Umgebung vertraut und die Sicherheit erhöht werden kann.

Es hat sich auch bewährt, wenn alle E/A-Einheiten, mit Ausnahme des Passworteingabegeräts, gesperrt sind und andere, im Computer laufende Programme gesperrt sind, während das Passwortleseprogramm ausgeführt und das Passwort empfangen wird.

Die Tatsache, dass das Passwortleseprogramm basierend auf der TCB ausgeführt wird, wird über ein Signal angezeigt. Während beispielsweise das Passwortleseprogramm das Passwort empfängt, zeigt eine LED einen sicheren Eingabemodus an. Der Benutzer wird so informiert, dass er das Passwort in das richtige Programm eingibt.

Wird das programm-/passwortspezifische Identifizierungszeichen von dem programmspezifischen Identifizierungszeichen, dem empfangenen Passwort und einem zusätzlichen Wert errechnet, dann hat das den Vorteil, dass dieses programm-/passwortspezifische Identifizierungszeichen das Gerät oder den Computer angibt, in dem das programm-/passwortspezifische Identifizierungszeichen erzeugt wird. Wenn jemand die Passworteingabe beobachtet und das Passwort wissen möchte, dann kann dieses Passwort jedoch nicht in einem anderen Gerät oder Computer benutzt werden.

Es ist möglich, das programm-/passwortspezifische Identifizierungszeichen als Schlüssel zu benutzen, um ein anderes Programm zu entschlüsseln. Da das programm-/passwortspezifische Identifizierungszeichen ein im wesentlichen einzigartiger Wert ist, ist der Schlüssel sicher und kann nur von dem Gerät des Benutzers erzeugt werden.

In die Trusted Computing Base sollte ein Hash-Funktionsgenerator eingesetzt werden, so dass das programmspezifische Identifizierungszeichen und das programm-/passwortspezifische Identifizierungszeichen abgeleitet und so für die Trusted Computing Base automatisch bereitgestellt werden. Ausgehend von der grundlegenden Sicherheitspolitik kann die Trusted Computing Base von einem Angreifer weder umgangen noch unterlaufen werden.

BESCHREIBUNG DER ZEICHNUNGEN

Die Erfindung wird nachfolgend detailliert mit Bezug auf die beiliegenden, schematischen Zeichnungen beschrieben, wobei:

Fig. 1 ein Blockdiagramm von einem Computersystem gemäß der vorliegenden Erfindung zeigt;

Fig. 2 eine schematische Darstellung von einer Passworteingabe gemäß der vorliegenden Erfindung zeigt, und

Fig. 3 eine schematische Darstellung von einer anderen Passworteingabe zeigt, in die ein heimtückisches Programm verwickelt ist.

Alle Figuren sind zum Zwecke der Klarheit weder mit ihren tatsächlichen Maßen abgebildet noch sind die Beziehungen zwischen den Maßen in einem realistischen Maßstab dargestellt.

DETAILLIERTE BESCHREIBUNG DER ERFINDUNG

Es wird allgemein auf die Figuren und speziell auf **Fig.** 1 Bezug genommen, wobei die wesentlichen Funktionsmerkmale eines sicheren Passworteingabesystems für Computer mittels kryptographischer Funktionen nachstehend ausführlicher beschrieben ist. Zuerst werden einige allgemeine Punkte behandelt.

Hash-Funktion

Eine Hash-Funktion ist eine wirksame Computerfunktion, um binäre Zeichenketten von beliebiger Länge als binäre Zeichenketten von fester Länge abzubilden.

One-Way-Hash-Funktion

Eine One-Way-Hash-Funktion ist eine Funktion, die eine Meldung von variabler Länge nimmt und einen Festlängen-Hash oder Festlängenwert errechnet. Somit ist h = H(M), wobei H die One-Way-Hash-Funktion ist, M die Meldung und h der Hash-Wert für die Meldung M ist. Mit Hash h ist es rechnerisch nicht möglich, eine Meldung M mit diesem Hash zu finden. Mit diesem Hash kann man tatsächlich keine brauchbaren Informationen über eine Meldung M finden. Bei einigen One-Way-Hash-Funktionen ist es auch rechnerisch unmöglich, zwei Meldungen zu finden, die denselben Hash erzeugen. Eine One-Way-Hash-Funktion kann außerdem geheim oder öffentlich sein, genau wie eine Verschlüsselungsfunktion. MD5, SHA-1 und Snefru sind Beispiele von öffentlichen One-Way-Hash-Funktionen.

Wird eine solche One-Way-Hash-Funktion auf ein Programm E angelegt, das irgendein Programm sein kann, dann ist die Ausgabeg der Hash-Wert h, ein im wesentlichen einzigartiger Wert, der auch programmspezifisches Identifizierungszeichen genannt wird. Dieses programmspezifische Identifizierungszeichen kann auch als Name betrachtet werden, der dem spezifischen Programm E gegeben wird. Anders ausgedrückt, kann das Programm E, das als Bytestrom $E = (b_0, b_1, b_2$ usw.) angezeigt werden kann, seinem im wesentlichen einzigartigen Namen H(E) zugeordnet werden. Somit läuft das Programm E unter dem Label H(E). Auf vorhandene Daten, die vom Programm E erstellt wurden, kann nur im Programm E zugegriffen werden, und sie tragen auch den Namen oder das programmspezifische Identifizierungszeichen H(E).

Wird beispielsweise die oben erwähnte One-Way-Hash-Funktion SHA-1 benutzt, liegt die Wahrscheinlichkeit, zwei identische programmspezifische Identifizierungszeichen zu finden, bei etwa 1 bis 2^{80}, und die Wahrscheinlichkeit, in einem bestimmten Programm ein anderes Programm mit demselben programmspezifischen Identifizierungszeichen zu finden, bei ca. 1 bis 2^{160}.

Trojanische Pferde

Benutzer geraten normalerweise durch das Herunterladen eines Programms, beispielsweise aus dem Internet, das sicher zu sein scheint oder dem Benutzer zum Beispiel freie Onlinezeit verspricht, an die sogenannten Trojanischen Pferde. Sobald es heruntergeladen ist und ausgeführt wird, beginnt der heimtückische Code zu arbeiten. Der Unterschied zwischen Trojanischen Pferden und herkömmlichen Computerviren ist, dass sich die Trojanischen Pferde nicht von alleine wiederholen oder verbreiten. Sie können nur absichtlich über E-Mail oder Diskette übertragen oder direkt auf einen PC heruntergeladen werden. Das heißt, dass, anders als bei herkömmlichen Computerviren, die Benutzer normalerweise nur von einem spezifischen Trojanischen Pferd betroffen sind. Dadurch kann aber in bezug auf die Sicherheit und den Verlust von Daten ein großer Schaden verursacht werden.

Trusted Computing Base (TCB)

Unter Trusted Computing Base, kurz TCB genannt, versteht man die Gesamtheit der Schutzmechanismen innerhalb

eines Computersystems, einschließlich Hardware, Firmware und Software, die in der Kombination für die Unterstützung einer Sicherheitsstrategie verantwortlich sind. Teil der Trusted Computing Base ist ein Betriebssystem. Die Sicherheitsstrategie verlangt, dass die Trusted Computing Base weder umgangen noch unterlaufen werden kann, d. h. sie ist vor Angriffen sicher.

Das vorliegende sichere Passworteingabesystem kann im allgemeinen in Computern und Computersystemen benutzt werden. Wenn auf einen Computer Bezug genommen wird, ist irgendein Gerät gemeint, das Teil eines lokalen Netzwerks sein kann. Zum Beispiel die folgenden Geräte: Laptops, Workpads, Notepads, persönliche digitale Assistenten (PADs), Notebooks und sonstige tragbaren Computer, Tischgeräte, Computerterminals, Netzwerkcomputer, Internetterminals und sonstige Computersysteme, Set-Top-Boxen, Registrierkassen, Streifencodescanner, Kassenterminals, Auskunftssysteme, Mobiltelefone, Pager, Armbanduhren, Digitaluhren, Ausweise, Chipkarten und sonstige Handgeräte und integrierte Geräte. Weitere Geräte, die berücksichtigt wurden, sind enthalten in: Kopfhörern, Human Interface Device (HID), passenden Peripheriegeräten, Daten- und Sprachzugriffspunkten, Kameras, Druckern, Faxgeräten, Tastaturen, Joysticks, Küchengeräten, Werkzeugen, Sensoren wie beispielsweise Rauch- bzw. Brandmeldern und praktisch in sonstigen digitalen Einheiten.

Weitere Beispiele für tragbare Computer, die in Verbindung mit der vorliegenden Erfindung benutzt werden können, ist persönliches Eigentum, das mit computerähnlicher Hardware ausgerüstet ist, wie beispielsweise ein elektronisches Portemonnaie ("Smart Wallet"-Computer), Schmuck oder Kleidungsstücke. Außer einem elektronischen Portemonnaie gibt es eine Reihe verschiedener tragbarer Computer. Ein Beispiel für die Vielfalt an tragbaren Computern ist ein "Gürtel"-Computer ("belt" computer), mit dem der Benutzer surfen, diktieren und Dokumente bearbeiten kann, während er unterwegs ist. Ein weiteres Beispiel ist ein Kindercomputer, der mit einem persönlichen digitalen Assistenten für Grundschulkinder vergleichbar ist. Der Kindercomputer kann Aufgaben enthalten, Rechenaufgaben durchführen und Kindern helfen, ihre Hausaufgaben zu verwalten. Er kann mit anderen Kindercomputern verbunden werden, um die Zusammenarbeit zu erleichtern, und er kann auf den Computer eines Lehrers zugreifen, um Aufgaben oder Rückmeldungen (Feedbacks) herunterzuladen. Ein tragbares Gerät, ein Bürogerät oder eine Büroanlage, ein Heimgerät oder eine Heimanlage, Systeme zum Einsatz in Fahrzeugen oder Systeme zur öffentlichen Nutzung (Verkaufsautomaten, Fahrscheinautomaten, automatisierte Kassiereinrichtungen usw.) können in Verbindung mit der vorliegenden Erfindung benutzt werden.

Zum Verständnis der vorliegenden Erfindung zeigt **Fig.** 1 ein Blockdiagramm auf hoher Ebene von einem Computer **2**.

Der Computer **2** enthält Hardwarekomponenten **4**, zum Beispiel eine oder mehrere Zentraleinheiten (CPU) **6**, ein Direktzugriffsspeicher (RAM) **8** und eine Ein-/Ausgabeschnittstelle (E/A) **10**. Der Computer **2** enthält auch ein Betriebssystem **20**, in das ein Generatormodul **22** eingebettet ist. Zahlreiche Peripheriegeräte sind an den Computer **2** angeschlossen, zum Beispiel Sekundärspeichereinheiten **12**, wie ein Magnetplattenlaufwerk, Eingabemittel **14** oder Geräte wie eine Tastatur, eine Maus, ein Touch Screen, ein Mikrofon oder ein IR- oder HF-Empfänger, Anzeigegeräte **16**, wie ein Monitor oder eine Flüssigkristallanzeige (LCD) und Ausgabegeräte **18** wie Drucker, oder IR- oder HF-Sender. Der Benutzer gibt ein Passwort p über die Eingabemittel **14** ein. An die Ein-/Ausgabegeräte **14**, **18** könnte auch ein Chipkartenlesegerät angeschlossen werden. Ein Programm **24**, das zur Eingabe eines Passworts auffordert und ein Empfänger **26**, auch Passwortleseprogramm **26** genannt, werden im Computer **2** ausgeführt. Anzeigemittel **28** sind an das Betriebssystem **20** angeschlossen und somit auch an das Passwortleseprogramm **26**, wobei nur das Betriebssystem **20**, d. h. die TCB, und das Passwortleseprogramm **26** die Anzeigemittel **28** kontrollieren können. Diese Anzeigemittel **28** informieren den Benutzer mit einem Signal, dass das Passwort in das richtige Programm eingegeben wurde. Eine Leuchtdiode **28**, auch LED **28** genannt, wäre geeignet, um dem Benutzer ein optisches Signal anzuzeigen. Es kann statt dessen jedes passende Signal verwendet werden.

Die Hardwarekomponenten **4** und das Betriebssystem **20** bilden eine Trusted Computing Base, die die Basis für eine sichere und verläßliche Berechnung bildet. In der Trusted Computing Base ist das Generatormodul **22** zur Erstellung von programmspezifischen Identifizierungszeichen implementiert. Dieses Generatormodul **22** ist im Grunde ein kryptographischer Funktionsgenerator **22**, der sowohl in der Software als auch in der Hardware implementiert werden kann. Da die Errechnung eines Hash-Werts mittels einer Hash-Funktion, vorzugsweise eine One-Way-Hash-Funktion wie oben beschrieben, für einen Prozessor nicht zeitaufwendig ist, ist hier der kryptographische Funktionsgenerator **22** im Betriebssystem **20** selbst implementiert. Jede kryptographische Funktion, die einen im wesentlichen einzigartigen Wert ausgibt, ist geeignet.

Der Struktur des Computers **2**, wie mit Bezug auf **Fig.** 1 beschrieben, ist als das eigentliche Gerät anzusehen, das in den folgenden Ausführungsbeispielen verwendet werden kann. Daher tragen dieselben Komponenten auch dieselben Referenznummern.

Es wird weiter auf **Fig.** 2 Bezug genommen, die ein Blockdiagramm auf hoher Ebene von einer Passworteingabe gemäß der vorliegenden Erfindung zeigt. Im Betriebssystem **20** läuft das Programm **24**, das die Eingabe eines Passworts verlangt und das Passwortleseprogramm **26**. Das Passwortleseprogramm **26** wird von der Trusted Computing Base bereitgestellt und empfängt das eingegebene Passwort p über die Eingabemittel **14**. Das Programm **24** ist über ein Netzwerk mit einer Bank **30** verbunden, die zu Beginn die Eingabe des Passworts verlangt. Ein transformiertes Passwort F[H(E), p] wurde bereits in der Bank **30** gespeichert. Nachdem die Bank **30** das transformierte Passwort F[H(E), p] angefordert hat, sendet das Programm **24** diese Anforderung an das Passwortleseprogramm **26**. Der Einfachheit halber ist das Generatormodul **22** in **Fig.** 2 nicht abgebildet, aber das programmspezifische Identifizierungszeichen H(E) und das programm-/passwortspezifische Identifizierungszeichen F[H(E), p] werden von dem Generatormodul **22** erzeugt und vom Betriebssystem **20** bereitgestellt. Das Programm **24** sendet eine Meldung einschließlich seines abgeleiteten programmspezifischen Identifizierungszeichens H(E) und die Anforderung oder die Anfrage für die bzw. nach der Passworteingabe an das Passwortleseprogramm **26**, was durch den mit H(E) ?p gekennzeichneten Pfeil dargestellt ist. Anders ausgedrückt: die Anforderung nach dem Passwort wird gesendet, wobei das Betriebssystem **20** das programmspezifische Identifizierungszeichen H(E), das durch Einsatz des Generatormoduls **22** abgeleitet wurde, und somit die oben erwähnte Hash-Funktion zu dem Programm **24** oder wenigstens einem Teil davon hinzufügt. Das Passwortleseprogramm **26** und das Betriebssystem **20** sorgen dann dafür, dass die LED **28** eingeschaltet wird, und alle E/A-Schnittstellen mit Ausnahme des Passworteingabegeräts **14** werden gesperrt, und die anderen laufenden Programme werden blockiert. Das Passwortleseprogramm **26** erlaubt jetzt, einen

Passwortwert oder das kurze Passwort p einzulesen. Danach, d. h. nachdem das Passwort p im Passwortleseprogramm **26** empfangen wurde, werden die Sperren aufgehoben, und die LED **28** wird ausgeschaltet. Das Generatormodul **22** wird auf das programmspezifische Identifizierungszeichen H(E) und das Passwort p angelegt, um das programm-/passwortspezifische Identifizierungszeichen F[H(E), p], auch transformiertes Passwort F[H(E), p] genannt, angelegt. Bei der Gelegenheit können auch Teile des programmspezifischen Identifizierungszeichens H(E) bzw. das Passwort p benutzt werden. Das transformierte Passwort F[H(E), p] wird dann vom Passwortleseprogramm **26** an das Programm **24** gesendet, was durch den mit F[H(E), p] gekennzeichneten Pfeil dargestellt ist und an die Bank **30** gesendet, wo es beispielsweise mit einem vorgespeicherten Passwort verglichen wird.

In einem weiteren Ausführungsbeispiel werden das programmspezifische Identifizierungszeichen H(E), das Passwort p und ein zusätzlicher Wert s – nicht in **Fig.** 2 abgebildet – von dem Generatormodul **22** transformiert oder umgerechnet. Dabei wird das transformierte Passwort F[H(E), p] gerätespezifisch. Das heißt, wenn jemand die Passworteingabe beobachtet und das Passwort kennt, kann er/sie dieses Passwort nicht in einem anderen Computer oder Gerät zum Anmelden benutzen.

Um das programmspezifische Identifizierungszeichen H(E) sowie das programm-/passwortspezifische Identifizierungszeichen F[H(E), p] zu erzeugen, kann im allgemeinen dieselbe kryptographische Funktion angewendet werden.

Fig. 3 zeigt eine schematische Darstellung von einer anderen Passworteingabe, bei der ein heimtückisches Programm B beteiligt ist. **Fig.** 3 zeigt ein Personal Device **2**, beispielsweise den Computer wie er mit Bezug auf **Fig.** 1 beschrieben wurde, der an ein Programm A angeschlossen ist, das in einer Bank **30** läuft, und das heimtückische Programm, das bei einem Knacker **32** läuft. **Fig.** 3 zeigt eine erste Trusted Computing Base, TCB_A, die das Personal Device **2** und das Programm A enthält, und eine zweite Trusted Computing Base, TCB_B, die das Personal Device **2** und das heimtückische Programm B enthält. Das Personal Device **2** ist mit der LED **28** ausgerüstet, um die sichere Passworteingabe anzuzeigen. In diesem Beispiel liegen die Programme A, B, die die Passworteingabe verlangen, außerhalb der Personal Device **2** und somit außerhalb der Trusted Computing Base. Wie aus **Fig.** 3 ersichtlich ist, sendet das Programm der Bank **30** eine Passwortanforderung getpw() zusammen mit seinem abgeleiteten programmspezifischen Identifizierungszeichen H(A) an das Personal Device **2**, wie dies durch den mit H(A), getpw() gekennzeichneten Pfeil angegeben ist. Das heimtückische Programm B von dem Knacker **32** verlangt andererseits auch ein Passwort, wie dies durch den mit H(A), getpw() gekennzeichneten Pfeil angegeben ist. Die Personal Device **2** sendet an die Bank **30** eine Meldung folgenden Inhalts H(D), H(H(A), p, s), wobei H(A) das programmspezifische Identifizierungszeichen des Programms A, p das eingegebene Passwort und s ein gerätespezifischer Wert von dem Generatormodul **22** mit der Funktion H transformiert oder umgerechnet werden, um das transformierte Passwort H(H(A), p, s) zu erzeugen. Zum Zwecke der Klarheit ist das Generatormodul **22** in **Fig.** 3 nicht abgebildet. Das geräte-/programmspezifische Identifizierungszeichen H(D) des Personal Device **2** wird zu dem transformierten Passwort H(H(A), p, s) hinzugefügt. Die Personal Device **2** sendet andererseits an den Knacker **32** eine Nachricht, die H(D), H(H(B), p, s) enthält, wobei H(B) das programmspezifische Identifizierungszeichen des heimtückischen Programms B, p das eingegebene Passwort und s der gerätespezifische Wert vom Generatormodul **22** wiederum mit der Funktion H transformiert oder umgerechnet werden, um das transformierte Passwort H(H(B), p, s) zu erzeugen. Es ist klar, dass, nachdem der Benutzer das Passwort p eingegeben hat, die transformierten Passwörter H(H(A), p, s) und H(H(B), p, s) nicht mehr dieselben sind. Da das transformierte Passwort H(H(B), p, s) nichts über das Passwort p selbst aussagt, und es unmöglich ist, das Passwort p aus H(H(B), p, s) zu berechnen, kann der Knacker **32** mit dem transformierten Passwort H(H(B), p, s) nichts anfangen. Die Tatsache, dass die Meldungen die jeweiligen programmspezifischen Identifizierungszeichen H(A), H(B), H(D) enthalten, kann benutzt werden, um die Gültigkeit von einem Programm zu einem anderen Programm zu überprüfen. Das gegenseitige Vertrauensverhältnis zwischen verschiedenen Programmen kann somit einfach eingerichtet werden. Das heißt beispielsweise, dass die Personal Device **2** eine Liste mit programmspezifischen Identifizierungszeichen hat, die vertrauenswürdig sind. Anforderungen von unbekannten Programmen oder Geräten können zurückgewiesen werden.

Ein beschriebenes Ausführungsbeispiel kann mit einem oder mit mehreren von den abgebildeten bzw. beschriebenen Ausführungsbeispielen kombiniert werden. Dies ist auch für ein Leistungsmerkmal oder mehrere Leistungsmerkmale von den Ausführungsbeispielen möglich.

Die vorliegende Erfindung kann in der Hardware, der Software oder in einer Kombination von Hardware und Software ausgeführt werden. Jede Art von Computersystem oder anderen Vorrichtungen, die zur Ausführung der hier beschriebenen Methoden entsprechend angepasst sind, ist geeignet. Eine typische Kombination von Hardware und Software könnte ein Mehrzweckcomputersystem mit einem Computerprogramm sein, das, wenn es geladen ist und ausgeführt wird, das Computersystem steuert, so dass es die hier beschriebenen Verfahren ausführen kann. Die vorliegende Erfindung kann auch in einem Computerprogrammprodukt eingebettet sein, das alle Leistungsmerkmale enthält, die die Implementierung der hier beschriebenen Verfahren ermöglichen, und die, wenn sie in einem Computersystem geladen sind, diese Verfahren ausführen können.

Computerprogrammittel oder Computerprogramme im vorliegenden Kontext bedeuten ein Ausdruck in einer Sprache, in einem Code oder in einer Notation von einem Satz Anweisungen, die ein System mit der Fähigkeit der Datenverarbeitung veranlassen, eine bestimmte Funktion entweder direkt oder nach einem der folgenden Ereignisse oder nach beiden auszuführen: a) Konvertierung in eine andere Sprache, einen anderen Code oder in eine andere Notation. b) Reproduktion in einer anderen Materialform.

Patentansprüche

1. Ein Verfahren zum Einlesen eines Passworts (p) nach einer Anforderung von einem Programm (E), wobei das Verfahren folgende Schritte enthält:
   - Empfangen eines programmspezifischen Identifizierungszeichens (H(E)) vom Programm (E);
   - Empfangen des Passworts (p);
   - Erzeugen eines programm-/passwortspezifischen Identifizierungszeichens (F(H(E), p)) aus wenigstens dem programmspezifischen Identifizierungszeichen (H(E)) und dem empfangenen Passwort (p) und
   - Senden des programm-/passwortspezifischen Identifizierungszeichens (F(H(E), p)) an das Programm (E) zu senden, wobei das programm-/passwortspezifische Identifizierungszeichen (F(H(E), p)) von dem Programm (E) verarbeitet werden kann.

2. Das Verfahren gemäß Anspruch 1, wobei
   - das programmspezifische Identifizierungszeichen (H(E)) abgeleitet wurde, indem eine erste kryptographische Funktion (H) auf wenigstens einen Teil des Codes von Programm (E) angewendet wurde, und
   - das programm-/passwortspezifische Identifizierungszeichen (F(H(E), p)) erzeugt wird, indem eine zweite kryptographische Funktion (F) auf das programmspezifische Identifizierungszeichen (H(E)) und auf wenigstens einen Teil des empfangenen Passworts (p) angewendet wird, wobei die erste kryptographische Funktion (H) bzw. die zweite kryptographische Funktion (F) eine Hash-Funktion enthält, vorzugsweise eine One-Way-Hash-Funktion, zum Beispiel MD5 oder SHA-1.

3. Das Verfahren gemäß Anspruch 1, wobei ein Passwortleseprogramm (**26**) und das programmspezifische Identifizierungszeichen (H(E)) mittels einer Trusted Computing Base (TCB) bereitgestellt werden, wobei beide vorzugsweise dieselbe Trusted Computing Base (TCB) benutzen.

4. Das Verfahren gemäß Anspruch 3, wobei das Passwort (p) im Passwortleseprogramm (**26**) empfangen wird, und alle E/A-Geräte während der Ausführung des Passwortleseprogramms (**26**) gesperrt und die anderen Programme während dieser Zeit blockiert werden.

5. Das Verfahren gemäß Anspruch 3, wobei die Tatsache, dass das Passwortleseprogramm (**26**) in der Trusted Computing Base (TCB) ausgeführt wird, über ein Signal angezeigt wird, was vorzugsweise über eine LED (**28**) erfolgt, die aufleuchtet, während das Passwortleseprogramm (**26**) das Passwort (p) empfängt.

6. Das Verfahren gemäß Anspruch 1, wobei das programm-/passwortspezifische Identifizierungszeichen (F(H(E), p, s)) von dem programmspezifischen Identifizierungszeichen (H(E)), dem empfangenen Passwort (p) und einem zusätzlichen Wert (s) erzeugt wird, wobei der zusätzliche Wert (s) ein Gerät (**2**) kennzeichnet, in dem das programm-/passwortspezifische Identifizierungszeichen (F(H(E), p, s)) erzeugt wird.

7. Das Verfahren gemäß Anspruch 1, wobei das programm-/passwortspezifische Identifizierungskennzeichen (F(H(E), p)) als Schlüssel benutzt wird, um ein anderes Programm zu entschlüsseln.

8. Ein Computerprogramm, das Programmcodemittel enthält, um die Schritte gemäß einem der Ansprüche 1 bis 7 auszuführen, wenn das Programm in einem Computer läuft.

9. Ein Computerprogrammprodukt, das Programmcodemittel enthält, die in einem computerlesbaren Medium gespeichert sind, um das Verfahren gemäß einem der Ansprüche 1 bis 7 auszuführen, wenn das Programm in einem Computer läuft.

10. Eine Computereinheit (**2**) zum Einlesen eines Passworts (p) nach einer Anforderung von einem Programm (E) mit
   - Eingabemitteln (**14**) zur Eingabe des Passworts (p);
   - Empfängermitteln (**26**), um ein programmspezifisches Identifizierungszeichen (H(E)) und das Passwort (p) zu empfangen, und
   - einem Generatormodul (**22**), das an die Empfängermittel (**26**) angeschlossen ist, um ein programm-/passwortspezifisches Identifizierungszeichen (F(H(E), p)) von wenigstens dem eingegebenen Passwort (p) und dem programmspezifischen Identifizierungszeichen (H(E)) zu erzeugen, wobei das programm-/passwortspezifische Identifizierungszeichen (F(H(E), p)) von dem Programm (E) verarbeitet werden kann.

11. Die Computereinheit (**2**) gemäß Anspruch 10, wobei das Generatormodul (**22**) ein Hash-Funktionsgenerator ist, und das programmspezifische Identifizierungszeichen (H(E)) mittels des Generatormoduls (**22**) aus dem Programm (E) abgeleitet werden kann.

12. Die Computereinheit (**2**) gemäß Anspruch 10, die des weiteren eine Trusted Computing Base (TCB) und Anzeigemittel (**28**) enthält, die mit der Trusted Computing Base (TCB) verbunden sind.

13. Die Computereinheit (**2**) gemäß Anspruch 12, wobei das Anzeigemittel (**28**) ein Signal liefert, das einen sicheren Eingabemodus anzeigt, während ein Passwortleseprogramm (**26**), das von der Trusted Computing Base (TCB) bereitgestellt wird, ausführbar ist.

Hierzu 2 Seite(n) Zeichnungen

- Leerseite -

Nummer: DE 101 10 316 A1
Int. Cl.[7]: G 06 F 12/14
Offenlegungstag: 27. September 2001

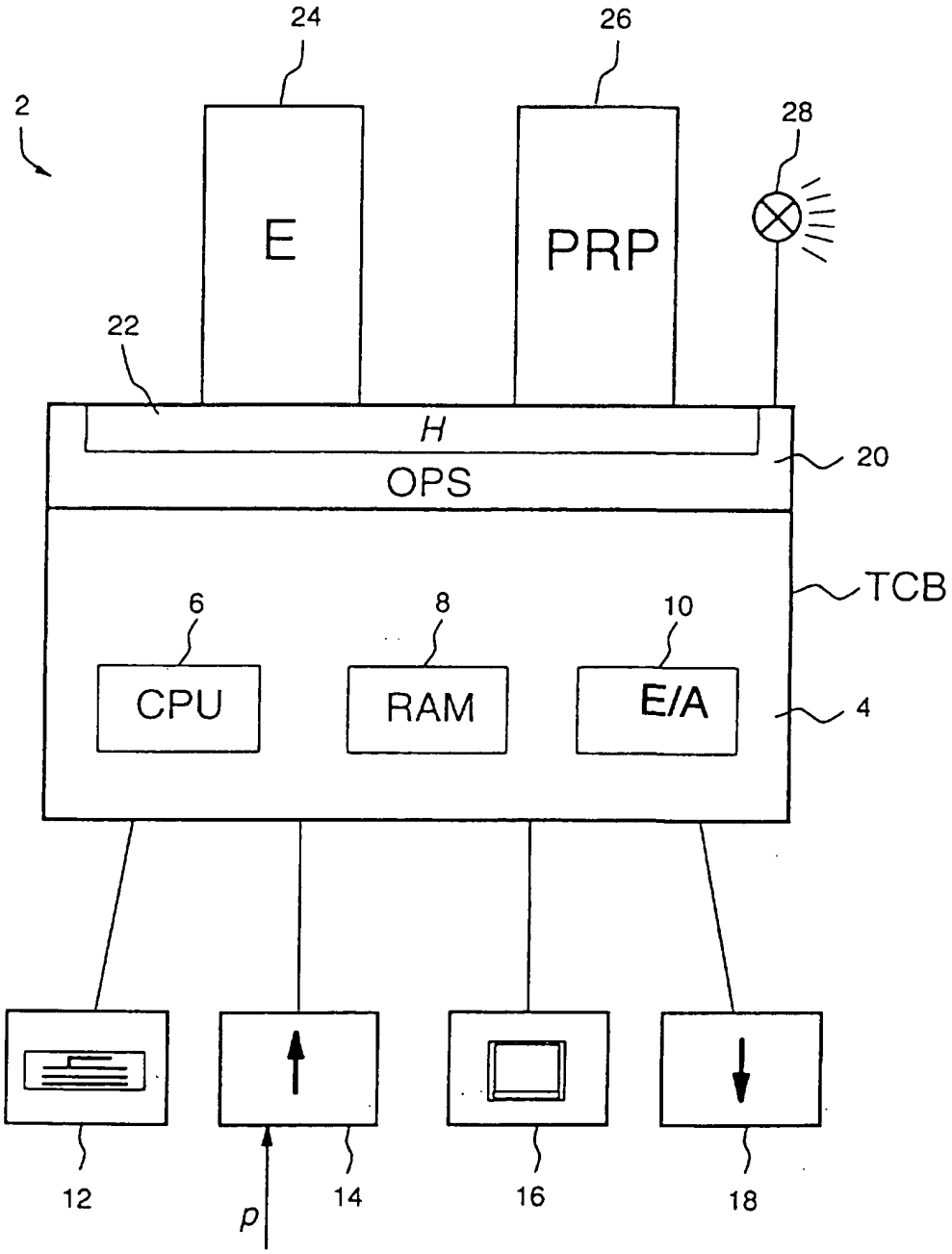


Fig. 1

Nummer: DE 101 10 316 A1
Int. Cl.[7]: G 06 F 12/14
Offenlegungstag: 27. September 2001

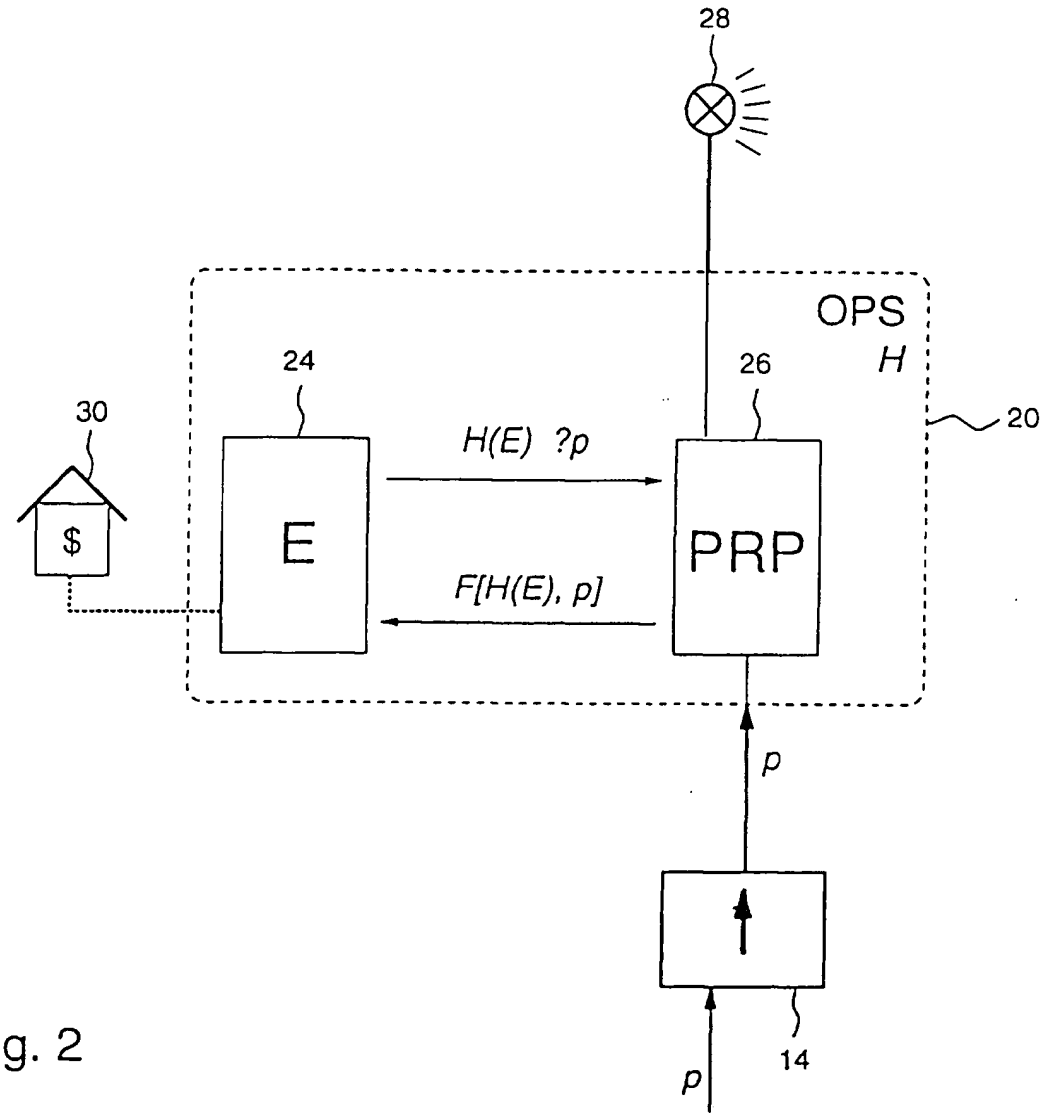


Fig. 2

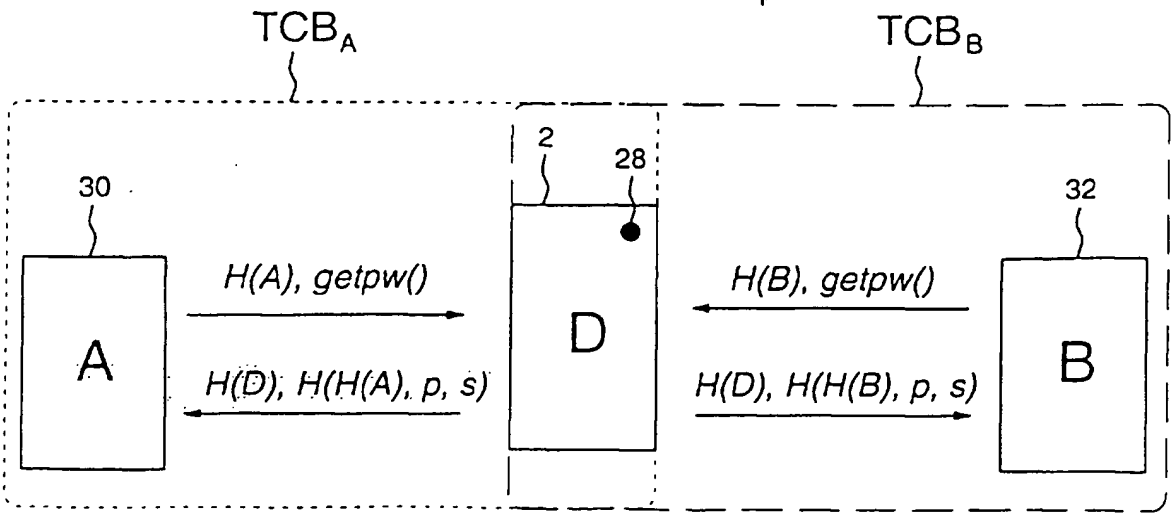


Fig. 3